Was brauchen wir als Zivilgesellschaft eigentlich für eine Art von Netzwerk und was für eine Technik hätten wir denn gerne?

Verschriftlichung des Vortrags von Christian Grothoff

„All governments should be pressured to correct their abuses of human rights." – Richard Stallman

Im Vortrag von Christian Grothoff wurden die politischen Anforderungskataloge für das GNU-Name-System und GNU-Taler vorgestellt. Danach wurde gezeigt, wie diese Anforderungen technisch umgesetzt wurden.

Was die Projekte, mit denen Grothoff sich beschäftigt, verbindet, ist der Wunsch nach einer liberalen Gesellschaft, der sich an vielen Stellen wiederfindet. In der Allgemeinen Erklärung der Menschenrechte steht im Artikel 12 „Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden." So ziemlich alle Nationen haben dieses Dokument ratifiziert und das sagt ganz klar, der Staat darf nicht in private Kommunikation eingreifen. Die ist ein schöner Anspruch, den man auch in einem Netzwerk haben sollte, so Grothoff.

Einen weiteren Anspruch, im sozialen Bereich, findet man in Artikel 22:

> *„Jeder hat (...) das Recht auf soziale Sicherheit und Anspruch darauf, (...) in den Genuss der wirtschaftlichen, sozialen und kulturellen Rechte zu gelangen, die für seine Würde und die freie Entwicklung seiner Persönlichkeit unentbehrlich sind."*

So wie Grothoff den Kapitalismus bisher erlebt hat, passiere die Umsetzung solcher Ansprüche nicht von alleine. Man benötigt einen Sozialstaat, der durchaus die Pflicht hat, in die Wirtschaft einzugreifen und dafür zu sorgen, dass allen zumindest eine gewisse gesellschaftliche Teilhabe möglich ist. Auf diese Grundwerte haben wir Menschen uns bis auf ein paar Ausnahmen global geeinigt – Sie stehen dementsprechend nicht zur Debatte. Was technisch heutzutage umgesetzt wird, findet seine Grenzen jedoch nicht durch politische Gesetze und Grundwerte. Der tiefe Staat macht, was er möchte und findet Grenzen nur noch darin, was die Technik erlaubt und was nicht. Das Internet wird weitestgehend überwacht, die technische Grenze dieser Überwachung ist Kryptographie. Kann diese nicht gebrochen werden, kann nicht überwacht werden, ansonsten wird es jedoch gemacht.

Ebenso hat es sich im Wirtschaftlichen entwickelt. Das Internet hat dafür gesorgt, dass die Wirtschaft globalisiert ist. Weil sich Konzerne und Firmen über staatliche Grenzen sehr leicht hinwegsetzen können, wird es dem Staat schwierig gemacht, sie zu kontrollieren. Insofern muss der Anspruch gestellt werden, dass die Technik dem Staat die Steuerungsmechanismen wieder in die Hand gibt, um die sozialen und freiheitlichen Ziele zu erreichen.

Die Realität sieht jedoch nicht danach aus. Von Edward Snowden haben wir gelernt, dass Briten und Amerikaner, wie man historisch schon gesehen haben kann, mit Hilfe von Überwachung

alles wissen und alles kontrollieren wollen. Auf der „corporate-sozialen Schiene" erkennt man es z. B. an Amazon. Ein massiv profitables Unternehmen, eines der größten der Welt, zahlte in Amerika im Jahr 2017 ‚null' Steuern.

Design-Ziele von GNUnet

So wie beschrieben kann es nicht bleiben, also muss von den InformatikerInnen, die für Technikentwicklung zuständig sind, eine Änderung kommen. Mit dem GNU-Projekt und insbesondere mit dem GNUnet-Projekt ist es der Anspruch, ein Netzwerk zu erschaffen, das besser ist und wird. Angefangen wurde dabei nicht etwa mit militärischen Zielen wie denen des DARPA-Netzes (siehe Vortrag von Yasha Levine auf Seite 33), sondern mit eigenen Zielen und Ansprüchen.

Da das GNUnet ein GNU-Projekt ist, ist der erste Anspruch natürlich, dass es als freie Software implementiert sein muss, nicht von irgendeiner Firma kontrolliert werden soll, sondern allen gehört. Das Grundkonzept ist *privacy-by-design*, wie es die DSGVO vorgibt. Es darf also nur die minimal notwendigen personenbezogenen Daten preisgeben. Es soll außerdem komplett verteilt und sowohl resistent gegen externe Angreifer als auch gegen böswillige Teilnehmer sein, da man davon ausgehen muss, dass nicht alle Leute wohlwollend sind. Es muss selbstorganisierend und nicht von Administratoren zentral verwaltet sein. Das Problem bei der Rolle der Administratoren ist, dass diese nicht nur die Macht über die Menschen haben, deren Strukturen sie verwalten, sondern es sie auch zu Zielpersonen werden lässt. Wenn Administratoren gehackt werden, dann trifft es im gleichen Zuge auch all diejenigen, die von ihnen ab-

Design-Ziele für zivile Netze

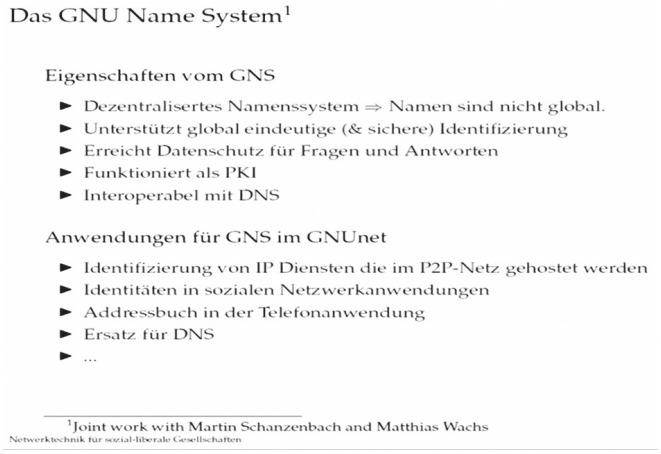
1. *GNUnet muss als Freie Software implementiert sein.*
2. *GNUnet darf nur die minimal notwendigen personenbezogenen Daten preisgeben.*
3. *GNUnet muss komplett verteilt und resistent sowohl gegen externe Angriffe als auch gegen bösartige Teilnehmer sein.*
4. *GNUnet muss selbstorganisierend und nicht von Administratoren oder zentraler Infrastruktur abhängig sein.*
5. *GNUnet muss den Benutzer informieren, wem vertraut werden muss, wenn private Kommunikationskanäle etabliert werden.*
6. *GNUnet muss ein offenes Netz sein, dem neue Peers beitreten können.*
7. *GNUnet muss ein breites Spektrum an Anwendungen und Geräten unterstützen.*
8. *GNUnet muss sensitive Daten durch Kompartimentierung schützen.*
9. *Die GNUnet-Architektur muss Ressourcen effizient einsetzen.*
10. *GNUnet muss Anreize schaffen, dass Peers mehr Ressourcen bereitstellen als sie selber verbrauchen.*

hängig sind. GNUnet will, dass idealerweise gar keine Administratoren mehr nötig sind und es selbstorganisierend ist. Die Idee ist, die eigene Hardware unter eigener Kontrolle zu haben und dann nichts weiter machen zu müssen. Anfragen an einen Administrator nach Accounts oder Passwörtern sollen dadurch unnötig werden.

Wenn ein sicherer Kommunikationskanal aufgebaut wird, kann es durchaus sein, dass dies über Infrastruktur Dritter geschieht, und vielleicht haben diese Dritten geholfen, einen Schlüssel zu verifizieren oder ähnliches. Wenn irgend jemandem vertraut werden muss, damit die eigene Kommunikation sicher ist, muss diese Tatsache bekannt gemacht werden. Es muss ein offenes Netz sein, das nicht einer kleinen, geschlossenen Community vorbehalten bleibt. Es sollen viele Anwendungen und Geräte unterstützt werden und es soll dafür gesorgt werden, dass die Daten nur dort vorliegen, wo sie wirklich benötigt werden, und nicht woanders. Ressourcen sollen effizient und damit umweltfreundlich eingesetzt werden, nicht etwa wie bei Bitcoin, für deren Betrieb enorme Mengen an Energie verbraucht werden. Und nicht zuletzt sollen Anreize gesetzt werden, dass Teilnehmende Ressourcen bereit stellen, damit das Netzwerk funktionieren kann und „freeloader" nicht einfach das Netz „DDOSsen" können. Die Design-Zielliste beinhaltet also sehr viel bezüglich Datenschutz und sehr viel zu Sicherheit und Verschlüsselung. Bei den Anforderungen fürs ARPANET fand man als einziges richtiges Sicherheitsziel etwas zu Verfügbarkeit – das Netz sollte lediglich ausfallsicher sein.

Für GNUnet wurden inzwischen verschiedene Anwendungen gebaut. Mit *Conversation* wurde ein sicheres, dezentrales Telefonieren implementiert. Es gibt Möglichkeiten für anonymes und nicht-anonymes Publizieren, ein IPv6–IPv4 Protokollübersetzer und Tunnel und viele andere Projekte, die auf dem GNUnet aufbauen. Es ist zu hoffen, dass die Liste noch viel länger wird. Zwei Anwendungen, nämlich das GNU-Name-System (GNS) ein zensurresistenter Ersatz für DNS und GNU-Taler, ein System für datenschutzfreundliches Bezahlen, sollen hier vorgestellt werden.

Das GNU-Name-System (GNS)



Das GNU-Name-System ist für das GNUnet ein zentraler Teil, genauso wie das Domain-Name-System (DNS) ein zentraler Teil für das Internet ist. Wenn DNS ausfällt, müssen IP-Adressen von Hand erfragt und eingetippt werden, das macht nur wenigen Freude.

Das GNU-Name-System ist im Gegensatz zum hierarchischen Namenssystem DNS ein dezentrales Namenssystem. Beim hierarchischen DNS sitzt ganz oben die ICANN, die z. B. die Top-Level-Domain *.de* an die DENIC oder *.ch* an die SWITCH vergibt. Die DENIC wiederum gibt Auskunft darüber dass, z. B. die Domain TU-Berlin.de von der TU in Berlin verwaltet wird. DNS ist also so durchhierarchisiert, dass umgesetzt werden könnte, das dem Administrator X aus Land Z die Rechte weggenommen werden können oder das ganze Land Z blockiert werden kann. Die Schweizer bauen als Teil ihres SCION Projektes an der ETH Zürich momentan ein System namens RAINS auf. Es soll ein nationales Netz entstehen, mit einem nationalen DNS, einer nationalen Zertifizierungsstelle und einer nationalen Blockierliste. Damit man „die ganzen Bösen" draußen halten kann, so Grothoff.

Wünscht man sich wie bei GNS nun ein dezentrales Namenssystem ohne Hierarchie, hat man den Nachteil, dass die Namen nicht mehr wirklich global sind. Man kann nun nicht mehr sagen, das der eine oder die andere bestimmt. Was man dabei aber trotzdem haben kann, sind eindeutige Identifizierer. Es handelt sich dabei dann jedoch nicht mehr um Namen, sondern genau genommen Public Keys. Diese sind nicht zwar nicht mehr leicht zu merken, aber es funktioniert.

Die wichtigste Eigenschaft neben der Dezentralisierung ist für Grothoff, dass Datenschutz für Anfragen und Antworten inner-

halb dieses Namenssystems umgesetzt wird. Dies geschieht auf eine Art und Weise, die man sich zunächst ersteinmal kaum vorstellen kann: Beim GNS ist es möglich, eine Frage nach der Auflösung eines Namens verschlüsselt zu stellen. Diese Anfrage kann an eine Gruppe gestellt werden, von der ein beliebiges Mitglied auf seiner Festplatte die Antwort gespeichert hat. Dieses Mitglied kann dabei zwar weder die Frage noch die Antwort entschlüsseln, kann aber mit Sicherheit sagen, dass die zur Verfügung stehende Antwort garantiert die Antwort auf die gestellte Frage ist, und kann die Antwort dann über Dritte weiterleiten. Auch alle Weiterleitenden können nur die verschlüsselte Frage und Antwort sehen, dabei aber verifizieren, dass die Antwort tatsächlich auf die Frage passt. Nur wer die Anfrage gestellt hat, kann die Antwort letzten Endes entschlüsseln. Es handelt sich dabei also um eine Art *Private Information Retrieval* – ein schöner kryptographischer Trick.

Da man auf diese Weise immer nur die richtigen Antworten bekommt, kann dieses Prinzip auch als *Public Key Infrastruktur* genutzt werden. Konzepte, die man von x.509, *Web of Trust*, DNSSec oder Ähnlichem kennt, können damit also nachgebildet werden. GNUnet hat das Verfahren sogar so gestaltet, dass es interoperabel mit DNS ist, so das es sogar einen Migrationspfad von DNS zu GNS gibt.

Vorstellbare Anwendungen sind das Adressieren beliebiger Dienste im *Peer-to-Peer*-Netz, Authentifizierung in sozialen Netzwerken oder Adressbücher. Ein Adressbuch der GNUnet-Telefonanwendungen ist z. B. im Wesentlichen eine Zone im GNU-Name-System. GNS könnte DNS somit langfristig ersetzen.

GNU-Taler

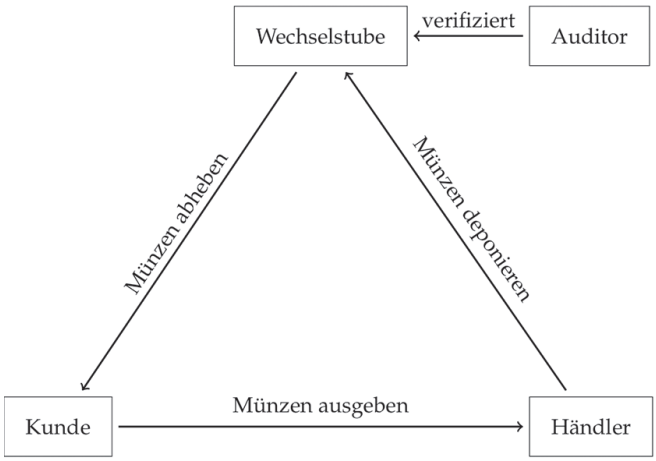
Nach den Grundsätzen des GNU-Projekts fehlte es außerdem auch an einem sozial orientierten Bezahlsystem, was Systeme, die hinter Buzzwörtern wie Blockchain und Bitcoin stehen, nicht leisten. Bestehende Systeme wie das Kreditkartensystem folgen dem Prinzip der Überwachung. Mit Kreditkarte kann man getrackt werden, egal wo man ist, ob man sich ein Busticket kauft, irgendwo essen geht oder ein Hotelzimmer bucht. Das ist unerwünscht und so entstand die Idee, etwas Bargeldähnliches digital, dabei aber auch sozial verträglich, nachzubauen.

Das GNU-Taler oder kurz Taler genannte System soll dafür sorgen, dass Einnahmen komplett transparent, Ausgaben jedoch komplett anonym bewerkstelligt werden. Zwar sollen Einkommen vom Staat gesehen werden, so dass Steuern drauf erhoben werden können oder festgestellt werden kann, wenn etwas nicht legal war. Der Staat soll in die Wirtschaft eingreifen können, aber gleichzeitig soll man Ausgaben komplett anonym machen können. Dieses Prinzip soll selbstverständlich als freie Software umgesetzt werden.

Die Designziele von Taler sind also anders als die aus der Parallelwelt der Blockchains und Cryptowährungen. Einige aus diesen Bereichen meinen, dafür zu sorgen, dass Einkommen besteuert werden können, sei eine unerwünschte Idee. Die Folge davon sind Menschen, die andere mit Crypto-Trojanern erpressen. Bei GNU-Taler wäre so etwas kaum möglich, da erpresstes Geld bei einer Steuerprüfung zum Vorschein kommen würde.

Der Staat soll also die Wirtschaft regulieren dürfen, dabei aber ansonsten nur die minimal notwendigen Daten verarbeiten. Dabei muss das System trotzdem einfach zu benutzen sein, da es sich sonst nicht durchsetzen würde. Es sollte außerdem effizient sein, da sonst wieder hohe – nicht nur finanzielle – Kosten entstehen.

Als Metapher ausgedrückt ergab sich daraus folgendes Prinzip für Taler: Wir haben eine Wechselstube, die mit der Bank interagiert, von der ich als Kunde Münzen abheben kann. Diese Münzen kann ich bei einem Händler ausgeben. Der Händler muss sie anschließend bei der Wechselstube deponieren und der Wechselstube Bescheid geben, dieses Geld gerade von einem Kunden bekommen zu haben. Der Händler weiß nicht, wer der Kunde war, da beim Bezahlen ein anonymer Kanal genutzt werden kann – zum Beispiel (aber natürlich nicht zwingend) Tor. Der Kunde muss sich beim Bezahlen also nicht identifizieren. Er gibt wie beim Bargeld dem Händler digitale Münzen, der sie aber nicht gleich zum Kaufen weiterbenutzen kann. Taler ist im Gegensatz zu Bargeld also nicht transitiv. Den Wert der Einnahmen kann der Händler nur wieder nutzen, wenn er es bei der Wechselstube einlöst, das Geld auf seinem Konto gutgeschrieben bekommt und für einen weiteren Kauf erneut abhebt. Taler soll nicht mit einer der bestehenden Cryptowährungen funktionieren, sondern mit ganz normaler Währung, wie Euro, Franken oder Dollar.

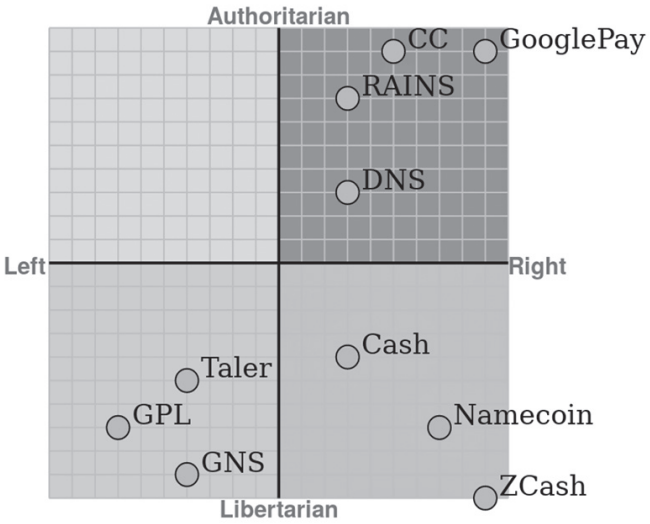


Eine Demo des Prinzips wurde auf der FIfFKon gezeigt und kann jederzeit unter *https://demo.taler.net* nachvollzogen werden: Auf der Website findet man ein kleines Ökosystem bestehend aus einer Bank, einigen Händlern. Mit wenigen Klicks ist dort ein Digitales Portemonnaie ein sogenanntes „Wallet" als Browser-Plug-In installiert und ein Bankkonto mit einem kleinen Startguthaben in der eigenen Währung KUDOS eröffnet. Bei der Bank kann man gegen eine kleine Gebühr einen gewünschten Betrag abheben, der dann nach der Eingabe einer TAN im Wallet im eigenen Browser landet und zuzüglich einer kleinen Gebühr vom Bankkonto abgezogen wird. Nun kann man sich aus der Bank ausloggen und sich über eine beliebige anonyme Verbindung auf die Website eines Händlers begeben, der etwas gegen Bezahlung anbietet. In der Demo handelt es sich um die fiktive Plattform „Essaystore" mit zu bezahlenden Artikeln. Will man sich nun, nach dem man den Teaser gelesen hat, einen Artikel vollständig zu Gemüte führen, ist nur ein Klick auf den Bezahlknopf nötig, und der Artikel ist aus dem digitalen Portemonnaie bezahlt und sofort freigeschaltet.

Alle die an Bezahlvorgänge mit Kreditkarten gewöhnt sind, sind an dieser Stelle überrascht, mit wie wenig Hindernissen und wie schnell das Bezahlen abläuft. Das ganze funktioniert, trotz Crypto, und selbst über langsame Netzanbindung, blitzschnell. Obendrein ist der ganze Bezahlvorgang überaus leicht zu verstehen. Letzten Endes wird diese Einfachheit beim Bezahlen nur durch die Crypto ermöglicht, da man eben nicht beim Bezahlen beweisen muss, wer man ist, sondern dies bereits beim Geldabheben geschehen ist. Beim Bezahlen muss nicht erst noch eine TAN per SMS eingetippt, ein Account erstellt, ein Gesicht in die Kamera gehalten werden oder dergleichen; man benötigt lediglich das eigene Endgerät, das das eigene abgehobene Geld verwaltet. Das Gerät signiert dann mit den eigenen Münzen und bezahlt.

Politische Einordnung

Wie in der Abbildung zu sehen ist, kann man die verschiedenen Bezahlsysteme politisch verorten.



Oben finden sich die autoritären Prinzipien: Kreditkarten, Militär, Google Pay, Schweizer Domain-Name-System – diese wollen die totale Kontrolle haben: Libertärer Kapitalismus ohne Regeln. Name-Coin ist der DNS-Ersatz für Blockchains. Dieses System ist nicht mehr autoritär, aber es ist sehr kapitalistisch gestaltet: Wer einen Namen haben will, muss zahlen. Rechts unten findet man ZCash, ein Bezahlsystem bei dem sowohl anonym ist, wer Geld bekommt als auch, wer bezahlt. ZCash beruht auf der Blockchain-Technik, ist sehr langsam, schlecht zu benutzen und sehr geeignet für kriminelle Aktivitäten. Grothoff findet sich politisch im Spektrum unten links wieder, und darum verortet er auch seine eigenen Projekte dort. GPL hält er für linkslibertär, so auch GNS und Taler. Leider gebe es in diesem Bereich noch zu wenig Technik.

GNS ist Cyberpeace

Bei einem Workshop zum Thema Cyberpeace traf Grothoff auf die „üblichen Leute von den Geheimdiensten", die der Meinung waren, Cyberpeace müsse irgendwo im oberen, also autoritären Bereich gemacht werden, und man Accountability bräuchte, um bei der Forensik feststellen zu können, wer es war, um dann „zurückschießen" zu können. Grothoff vertritt hingegen die Meinung, Cyberpeace mache man mit GNS, und eben gerade dadurch, dass man nicht mehr wisse, wer, würde eine Friedensgrundlage gelegt. GNS soll ein Allgemeingut – ein Commons – werden, das nicht irgendjemandem gehört, das allen gehört, das nicht einem Staat dient, einer Organisation, einer Firma oder einer Person, das nicht weiß, wem es dient. Es kann nicht sagen, was es es für eine Anfrage beantwortet hat, ob es eine deutsche, russische oder amerikanische Frage gelöst hat. Das kann es nicht wissen – die Crypto verhindert das. Wenn man Privatsphäre hat, hat man eine neutrale Infrastruktrur, deren Angriff keinen Sinn ergibt, weil man sich dabei selbst schadet, da man sie ja auch nutzt.

Spieltheoretisch, kann man, wenn man Accountability hat, immer sagen, man kann jemandem durch einen Angriff auf eine Sache schaden, die einem nicht selbst gehört. Wenn es aber allen gehört, so wie unsere Atmosphäre, greift man es nicht kriegerisch an. Da wären alle dagegen, da wir die Atmosphäre alle atmen.

Cyberpeace kommt also durch Privatsphäre. Wenn unbekannt bleibt, wer die Anfrage stellt, kann niemand mehr sagen, *dich* blockiere ich. Wenn unbekannt bleibt, für wessen Dienst ich eine Antwort speichere und weitergebe, kann ich demgegenüber nur neutral sein. Wenn alle die Infrastruktur nutzen, werden auch alle sie verteidigen. Wenn man hingegen dahingeht, etwas als die eigene Infrastruktur zu sehen, wie eine „Festung Europa", erst dann kann man sagen, ich grenze mich ab, dann kann man kriegerisch aktiv werden. Wenn wir Frieden haben wollen, bekommen wir das nur umgesetzt durch guten Datenschutz, Dezentralisierung und Commons. Und das heißt natürlich auch – durch freie Software.

Hinweis: Wer mehr über die Crypto von GNUnet und Taler erfahren will, findet Vorträge von Christian Grothoff auf media.ccc.de.

Christian Grothoff

Christian Grothoff, Softwarearchitekt, IT-Security, Privacy, GNUnet/GNU-Taler, ist Professor für Informatik an der Berner Fachhochschule. Er ist Ashoka Fellow und Maintainer von GNUnet.